UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,027	04/11/2001	Randall James Graham	MCVLT.001A	8350

20995 7590 03/01/2005

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/833,027	GRAHAM, RANDALL JAMES	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *44-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *44-66* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8/02, 11/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to request for consideration filed on November 17, 2004. Original application contained Claims 1 – 43. Claims 1 – 43 were cancelled. New Claims 44 – 66 were added. Therefore, presently pending claims are 44 – 66.

Information Disclosure Statement

2. Two initialed copies of the information disclosure statement, dated 08/06/2002 and 11/17/2004 are attached to this office action by the examiner.

Response to Arguments

3. Applicant's arguments filed on November 17, 2004, have been fully considered but they are not persuasive for the following reasons:

Applicant argued that the cited prior art (CPA) [Olkin et al. U.S. Patent number 6,584,564] does not teach, suggest or disclose, "a second security element interpretable by the recipient's browser to generate within the recipient browser a decryption key based upon the password and useable by the recipient's browser to decrypt the encrypted message for display within the recipient's browser".

Olkin teaches and describes a method for providing a security protection scheme for e-mail messages, which minimally burdens its users. The method is described with a detailed illustrative embodiment (Fig.1, 3, 7, 8 and Column 5 line 35 – Column 17 line 28), including the steps of encrypting a message using sender's information, providing sender and receiver information to encrypt and decrypt the message to form a secure e-mail message (Column 12 line 21 – Column 13 line 52 and Column 15 line 9 – Column 17 line 4). Olkin further teaches that the secure module (#26) that is installed in a browser (bother sender and receiver) generates (computes) an encryption and decryption (message) key based on password (sender and receiver) authentication, performing symmetric encryption and decryption using the same algorithm for both actions, e.g., Blowfish symmetric key encryption/decryption; performing secure hashing (Column 7 line 47 – Column 8 line 27 and Column 16 line 60 – Column 17 line 28).

Regarding newly added independent Claim 44, Olkin teaches and describes a secure electronic document including one or more self-contained security elements, wherein the secure electronic document and the one or more self-contained security elements are capable of being transmitted from a sender to a recipient (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), the secure electronic document comprising:

a first security element interpretable by a recipient's browser and capable of causing the recipient's browser to accept a password (Column 12 lines 21 – 56 and Column 15 lines 31 – 65),

Olkin teaches that the secure email (document) consists of sender's information and receiver's address, which prompts the receiver's browser to prompt for user's password;

an encrypted message (Column 12 line 21 – Column 13 line 52),

Olkin teaches that the sender is prompted for a password and authenticated, based on security policy choice, and the email message is encrypted; and

a second security element interpretable by the recipient's browser to generate within the recipient s browser a decryption key based upon the password, the decryption key being useable by the recipient's browser to decrypt the encrypted message for display within the recipient's browser (Column 12 lines 21 – 56, Column 15 lines 31 – 65 and Column 16 line 60 – Column 17 line 28),

Olkin teaches that the secure email message includes the email address of the sender whereby the recipient browser prompts and verifies the password based in part on association with the email address of the receiver and determines the receiver is authorized to generate the decryption key to decrypt the secure e-mail. If this authorization fails, the secure e-mail is not decrypted and the decryption key (message key) is not generated (Column 13 lines 7 – 67).

Regarding newly added independent Claim 58, Olkin teaches a method of sending a message to a recipient, the message including one or more self-contained security elements (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), the method comprising the steps of:

preparing an encrypted message by encrypting a source message using an encryption key and an encryption algorithm (Column 12 line 21 – Column 13 line 52 and Column 16 line 60 – Column 17 line 28), Olkin teaches that the sender provides an encryption key (message key) by prompting and verifying for user password based on security policy choice, and using symmetric key encryption/decryption algorithm, the email message is encrypted;

preparing a secure document comprising a first security element interpretable by a recipient's browser and capable of causing the recipient's browser to accept a password, a second security element interpretable by the recipient's browser to generate within the recipient's browser a decryption key based upon the password and useable by the recipient's browser to decrypt the encrypted message for display within the recipient's browser, and the encrypted message(Column 12 lines 21 – 56 and Column 15 lines 31 – 65),

Olkin teaches that the secure email (document) consists of sender's information and receiver's address, which prompts the receiver's browser to prompt for user's password; and

forwarding the secure document to an electronic system capable of delivering the secure document to a recipient (Column 6 lines 13 – 56 and Column 16 line 60 – Column 17 line 28),

Olkin teaches that the sender and receiver are registered with the security server (#24).

Applicant clearly has failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. Therefore, the examiner respectfully asserts that CPA does teach or suggest the subject matter broadly recited in independent new claims 44 and 58. Dependent claims 45 – 57 and 59 – 66 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action.

Accordingly, the rejection for the pending Claims 44 – 66 is respectfully maintained.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 44 – 66 are rejected under 35 U.S.C. 102(e) as being anticipated by Olkin et al. (Patent Number 6,584,564).

Regarding Claim 44, Olkin teaches and describes a secure electronic document including one or more self-contained security elements, wherein the secure electronic document and the one or more self-contained security elements are capable of being transmitted from a sender to a recipient (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), the secure electronic document comprising:

a first security element interpretable by a recipient's browser and capable of causing the recipient's browser to accept a password (Column 12 lines 21 – 56 and Column 15 lines 31 – 65),

Olkin teaches that the secure email (document) consists of sender's information and receiver's address, which prompts the receiver's browser to prompt for user's password;

an encrypted message (Column 12 line 21 – Column 13 line 52),

Olkin teaches that the sender is prompted for a password and authenticated, based on security policy choice, and the email message is encrypted; and

a second security element interpretable by the recipient's browser to generate within the recipient s browser a decryption key based upon the password, the decryption key being useable by the recipient's browser to decrypt the encrypted message for display within the recipient's browser (Column 12 lines 21 – 56, Column 15 lines 31 – 65 and Column 16 line 60 – Column 17 line 28),

Olkin teaches that the secure email message includes the email address of the sender whereby the recipient browser prompts and verifies the password based in part on association with the email address of the receiver and determines the receiver is authorized to generate the decryption key to decrypt the secure e-mail. If this authorization fails, the secure e-mail is not decrypted and the decryption key (message key) is not generated (Column 13 lines 7 – 67).

Regarding Claim 58, Olkin teaches a method of sending a message to a recipient, the message including one or more self-contained security elements (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), the method comprising the steps of:

preparing an encrypted message by encrypting a source message using an encryption key and an encryption algorithm (Column 12 line 21 – Column 13 line 52 and Column 16 line 60 – Column 17 line 28), Olkin teaches that the sender provides an encryption key (message key) by prompting and verifying for user password based on security policy choice, and using symmetric key encryption/decryption algorithm, the email message is encrypted;

preparing a secure document comprising a first security element interpretable by a recipient's browser and capable of causing the recipient's browser to accept a password, a second security element interpretable by the recipient's browser to generate within the recipient's browser a decryption key based upon the password and useable by the recipient's browser to decrypt the encrypted message for display within the recipient's browser, and the encrypted message(Column 12 lines 21 – 56 and Column 15 lines 31 – 65),

Olkin teaches that the secure email (document) consists of sender's information and receiver's address, which prompts the receiver's browser to prompt for user's password; and

forwarding the secure document to an electronic system capable of delivering the secure document to a recipient (Column 6 lines 13 – 56 and Column 16 line 60 – Column 17 line 28),

Olkin teaches that the sender and receiver are registered with the security server (#24).

Claim 45 is rejected as applied above in rejecting claim 44. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the recipient's browser comprises an HTML-compliant web browser (Column 15 lines 31 – Column 17 line 4).

Claim 46 is rejected as applied above in rejecting claim 44. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein said first security element comprises a form (Column 3 lines 42 – 50 and Column 15 lines 1 – 44).

Claim 47 is rejected as applied above in rejecting claim 44. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the recipient's browser Is configured to present a password entry 5eld and a decryption button when the first security element is processed by the recipient's browser (Column 3 lines 42 – 50 and Column 15 lines 1 – 44).

Claim 48 is rejected as applied above in rejecting claim 44. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the encrypted message comprises an email attachment (Column 13 line 7 – Column 14 line 35).

Claim 49 is rejected as applied above in rejecting claim 44. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein said second security element comprises a decryption element (Column 15 line 31 – Column 17 line 4).

Claims 50 and 60 are rejected as applied above in rejecting claims 44 and 58. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the second security element comprises script code configured to be processed by the recipient's browser (Column 7 line 47 – Column 8 line 67).

Claim 51 is rejected as applied above in rejecting claim 50. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the second security element further comprises JavaScript commands (Column 7 line 47 – Column 8 line 67).

Claim 52 is rejected as applied above in rejecting claim 50. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the second security element further comprises a set of Visual Basic script commands (Column 7 line 47 – Column 8 line 67).

Claim 53 is rejected as applied above in rejecting claim 44. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the second security element comprises an Active X control (Column 15 lines 9 – 15 and Column 18 line 60 – Column 19 line 6).

Claim 54 is rejected as applied above in rejecting claim 44. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the second security element comprises software that is configured to be processed by the recipient's browser (Column 7 line 47 – Column 8 line 67).

Claim 55 is rejected as applied above in rejecting claim 44. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the second security element is downloaded across a communications medium (Column 7 line 47 – Column 8 line 67).

Claim 56 is rejected as applied above in rejecting claim 44. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the second security element comprises a Java applet (Column 7 line 47 – Column 8 line 67).

Claim 57 is rejected as applied above in rejecting claim 44. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), where the second security element comprises both a Java program and an Active X control (Column 7 line 47 – Column 8 line 67).

Claim 59 is rejected as applied above in rejecting claim 44. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the first security element comprises an HTML-compliant wrapper (Column 9 lines 48 – 64 and Column 7 line 47 – Column 8 line 67).

Claim 61 is rejected as applied above in rejecting claim 60. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the processing script contains instructions for accessing the encrypted message (Column 12 lines 36 – 56).

Claim 62 is rejected as applied above in rejecting claim 58. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the second security element comprises a decryption element (Column 15 line 32 – Column 17 line 4).

Claims 63 and 66 are rejected as applied above in rejecting claim 58. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the source message is capable of being received as part of an XML template (Column 12 lines 57 – 65).

Claim 64 is rejected as applied above in rejecting claim 58. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the encryption key is capable of being derived from the password (Column 12 lines 36 – 49 and Column 16 line 60 – Column 17 line 28).

Claim 65 is rejected as applied above in rejecting claim 64. Furthermore, Olkin teaches and describes, a secure electronic document (Fig.1, 3, 7, 8; Summary, and Column 5 line 35 – Column 17 line 28), wherein the password is capable of being hashed to generate the encryption key (Column 12 lines 36 – 49 and Column 16 line 60 – Column 17 line 28).

Conclusion

4. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
February 14, 2005.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100